ABSTRACT

A method for automatic permission management in centralized and distributed operating systems using role-based access control that supports selective and multiple instantiations of roles, multiple inheritance of permission and membership, and provides scalable and efficient distribution, review, and revocation of permissions and access authorization.

The present invention provides, in a further aspect, automatic propagation of updates of role-permission hierarchies to the access control lists of all objects affected by such updates. The present invention provides, in yet a further aspect, per-role and per user review of permissions and requires neither redundant storage and additional administrative actions nor exhaustive searches of system resources. This invention makes use, in yet a further aspect, of both local and global groups for the instantiation of roles on multiple computer hosts, to implement nested groups and to enable the integration of extant host computers, which include local user accounts and groups defined on independent servers and workstations, within large distributed operating systems. In yet a further aspect, this invention provides the transition from an extant system state to an RBAC system state whereby permissions of users and groups to objects are managed centrally and automatically using roles, and removes the redundant user permissions to objects of a given state in the transition to the RBAC state.